حملات کانال جانبی تهدید بزرگی برای امنیت دستگاه‌های نهفته محسوب می‌شوند. در این گونه حملات با استفاده از اطلاعات جانبی نشتی از دستگاه مانند مصرف توان یا تشعشع الکترومغناطیس آن و استراتژی "تفرقه بیانداز و حکومت کن" بخش‌های مختلف کلید به‌دست می‌آید. پیش پردازش سیگنال‌های مشاهده شده اهمیت بالایی برای بهبود کیفیت حمله دارد. تاکنون روش های گوناگون فیلترینگ، تحلیل مولفه‌های اصلی و ...، برای ترکیب نمونه‌های مشاهده‌شده از یک متغیر هدف برای کاهش نویز در این سیگنال‌ها مطرح شده‌است، اما بهینه بودن این روش ها به ندرت اثبات می-شود. ما مدلی ریاضی از نشت چند نمونه همزمان از یک متغیر هدف در نویز نرمال ارائه می‌کنیم و فیلتر خطی بهینه برای کاهش نسبت سیگنال به نویز در این مدل را معرفی می‌کنیم. صحت عملکرد فیلتر با شبیه‌سازی و داده‌های واقعی تجربی اندازه‌گیری شده از مصرف توان دو میکروکنترلر مختلف بررسی می‌شود و کارآیی بهتر آن نسبت به روشهای پیش‌پردازش پیشرو موجود بررسی می‌شود. علاوه بر پیش‌پردازش ترکیب اطلاعات به دست آمده از متغیرهای هدف جداگانه نیز می‌تواند تاثیر چشمگیری در افزایش خطر تهاجم داشته باشد. هنگام مورد حمله قرار گرفتن الگوریتم AES عموما خروجی تابع SBOX به دلیل غیرخطی بود آن به عنوان متغیر هدف در نظر گرفته می‌شود. ما روشی مبتنی بر احتمال خطا و ساختار تابع ADDROUNDKEY برای ترکیب خروجی آن با تابع SBOX معرفی می‌کنیم که باعث بهبود قابل توجه در قدرت حمله می‌شود. همچنین اضافه‌کردن متغیرهای هدف از بخش‌های گوناگون فرایند MIXCOLUMNS از منظر میزان اطلاعاتی که برای ما به ارمغان می‌آورد، به صورت تجربی بررسی می‌شود. عملکرد روش‌های معرفی شده برای ترکیب خروجی چند متغیر هدف نیز با شبیه‌سازی و داده‌های واقعی تجربی بررسی می‌شود.